CLAIMS

What is claimed is:

1. A method of encrypting an electronic document which is open in an application program running in a general purpose computer, the general purpose computer including a display, a user input device, and a processor, the method comprising:

(a) from within the application program, the user issuing one of a "close," "save" or "save as" command for the document using the user input device;

(b) translating the command into an event;

(c) a crypto module trapping the event;

(d) the crypto module obtaining an encryption key value;

(e) the crypto module encrypting the document using the encryption key value;

(f) the crypto module passing control to an electronic document management system; and

(g) the electronic document management system executing the issued "close," "save" or "save as" command;

whereby the electronic document is automatically encrypted without making a display on the display.

2. A method of encrypting a document as set forth in claim 1 wherein the electronic document management system comprises a SQL database, a SQL database server and a SQL database client, the SQL database client being disposed in the general purpose computer.

3. A method of encrypting a document as set forth in claim 1 where step (d) comprises the steps of the crypto module determining if the document should be encrypted, and if not, then skipping step (e), and if so, then:

the crypto module retrieving an encryption key name associated with the document; and

the crypto module retrieving the encryption key value associated with the encryption key name.

4. A method of encrypting a document as set forth in claim 3, wherein there are plural encryption key values and at least one encryption key value is associated with the user, the method further comprising the steps of:

the user submitting to an access module for user authentication;

if the access module does not authenticate the user, then always skipping steps (d) and (e);

else in step (d), the crypto module retrieving the encryption key value associated with the encryption key name and the user.

5. A method of encrypting a document as set forth in claim 4, the general purpose computer further comprising a data reader device for reading user identification and encryption key values from a portable data storage device, the method further comprising the user presenting the portable data storage device to the data reader device, wherein the access module utilizes information stored in the portable data storage device to authenticate the user, and the encryption key value associated with the user is stored in the portable data storage device.

6. A method of encrypting a document as set forth in claim 5, wherein the data reader device comprises a smart card reader and the portable data storage device comprises a smart card.

7. A method of encrypting a document as set forth in claim 5, wherein the data reader device comprises a biometric recognition system and the portable data storage device comprises the user, wherein the access module utilizes unique information about the user for authentication, and the encryption key value is derived from at least one characteristic of the user.

8. A method of encrypting a document as set forth in claim 1 wherein the electronic document management system comprises a database, the database including an indicator of whether the document should be encrypted, and step (c) further comprises, if the indicator in the database does not indicate that the document is to be encrypted, then skipping steps (d) and (e).

9. A method of encrypting a document as set forth in claim 8, wherein if the indicator in the database does not indicate that the document is to be encrypted, then also skipping steps (f) and (g).

10. A method of encrypting a document as set forth in claim 1 wherein the general purpose computer comprises a workstation, and there is further provided a file server, wherein the crypto module comprises a crypto server on the workstation, the access module comprises an access server on the file server and an access client on the workstation, and the electronic document management system comprises an EDM database on the file server, an EDM server on the file server, and an EDM client on the workstation.

11. A method of encrypting a document as set forth in claim 1 wherein the operating system includes at least part of the electronic document management system.

12. A method of decrypting a document which is to be opened in an application program running in a general purpose computer, the general purpose computer including a display, user input device and a processor, the method comprising:

(a) the user selecting the document to be opened in the application program using the user input device;

(b) an "open" command issuing for the document to be opened in the application program;

(c) translating the command into an event;

(d) a crypto module trapping the event;

(e) the crypto module retrieving a decryption key value;

(f) the crypto module decrypting the document using the decryption key value;

(g) the crypto module passing control to an electronic document management system; and

(h) the electronic document management system executing the issued "open" command so that the document is opened in the application program;

whereby the document is automatically decrypted without making a display on the display.

13. A method of encrypting a document as set forth in claim 12 wherein the electronic document management system comprises a SQL database, a SQL database server and a SQL database client, the SQL database client being disposed in the general purpose computer.

14. A method of decrypting a document as set forth in claim 12 wherein step (e) comprises the crypto module determining if the document should be decrypted, and if not, then skipping step (f), and if so, then:

the crypto module retrieving a decryption key name associated with the document; and

the crypto module retrieving the decryption key value associated with the decryption key name.

15. A method of decrypting a document as set forth in claim 14, wherein there are plural decryption key values and at least one decryption key value is associated with the user, the method further comprising the steps of:

the user submitting to an access module for user authentication;

if the access module does not authenticate the user, then always skipping steps (e) and (f);

else in step (e), the crypto module retrieving the decryption key value associated with the decryption key name and the user.

16. A method of decrypting a document as set forth in claim 15, the general purpose computer further comprising a data reader device for reading user identification and decryption key values from a portable data storage device, the method further comprising the user presenting the portable data storage device to the data reader device, wherein the access module utilizes

information stored in the portable data storage device to authenticate the user, and the decryption key value associated with the user is stored in the portable data storage device.

17. A method of decrypting a document as set forth in claim 16, wherein the data reader device comprises a smart card reader and the portable data storage device comprises a smart card.

18. A method of encrypting a document as set forth in claim 16, wherein the data reader device comprises a biometric recognition system and the portable data storage device comprises the user, wherein the access module utilizes unique information about the user for authentication, and the decryption key value is derived from at least one characteristic of the user.

19. A method of encrypting a document as set forth in claim 12 wherein the electronic document management system comprises a database, the database including an indicator of whether the document should be decrypted, and step (d) further comprises, if the indicator in the database does not indicate that the document is to be decrypted, then skipping steps (e) and (f).

20. A method of encrypting a document as set forth in claim 19, wherein if the indicator in the database does not indicate that the document is to be decrypted, then also skipping steps (g) and (h).

21. A method of decrypting a document as set forth in claim 12 wherein the operating system includes at least a part of the electronic document management system.

22. A method of decrypting a document as set forth in claim 12 wherein the general purpose computer comprises a workstation, and there is further provided a file server, wherein the crypto module comprises a crypto server on the workstation, the access module comprises an access

server on the file server and an access client on the workstation, and the electronic document management system comprises an EDM database on the file server, an EDM server on the file server, and an EDM client on the workstation.

23. An electronic document management system for storing documents from an application in a workstation and retrieving documents from a file server to the application, the file server having a file system, the electronic document management system comprising:

(a) an access server in the file server comprising software for handling user authentication and file system access control for the file server;

(b) an access client in the workstation comprising software for enabling a user to sign on to the file server and obtain access to the file system on the file server;

(c) an EDM server in the file server comprising software for controlling an EDM database and EDM indexes to the EDM database;

(d) an EDM client in the workstation comprising software for interfacing the workstation to the EDM server and thereby allowing access by a user at the workstation to the EDM database; and

(e) a crypto server comprising software for intercepting I/O requests by the application and transparently handling encryption of the documents and decryption of encrypted documents;

wherein the access server and access client are functionally positioned between the EDM server and EDM client, and

the crypto server is functionally positioned between the application and the EDM client.

24. An electronic document management system as set forth in claim 23, wherein the crypto server software includes display commands, the display commands only for displaying error messages to the user.

25. An electronic document management system as set forth in claim 23, wherein the crypto server includes interfaces to plural cryptographic systems.

26. An electronic document management system as set forth in claim 25, the cryptographic systems comprising at least one of RSA, DES, Triple-DES, Blowfish, Triple Blowfish and IDEA.

27. An electronic document management system as set forth in claim 23, the workstation further comprising a data reader device for reading user identification and key values from a portable data storage device, wherein the access client utilizes information stored in the portable data storage device to authenticate the user, and the crypto server obtains key values for encrypting and decrypting the documents from the portable data storage device via the data reader device.

28. An electronic document management system as set forth in claim 27, wherein the data reader device comprises a smart card reader and the portable data storage device comprises a smart card.